BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-119
1 MARCH 1997

Communications and Information

★*ELECTRONIC MAIL (E-MAIL) MANAGEMENT AND USE*

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*, and establishes electronic mail (e-mail) manager and user duties and responsibilities.

It provides rules, standards, and guidance relating to the use of e-mail by the Air Force. Refer recommended changes or questions pertaining to this instruction to Headquarters United States Air Force (HQ USAF/SCXX). Refer conflicts between this and other instructions to the Headquarters Air Force Communications Agency (HQ AFCA/XPPD), 203 West Losey Street, Room 1065, Scott AFB IL 62225-5224, on AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ USAF/SCXX, 1250 Air Force Pentagon, Washington DC 20330-1250. Major commands (MAJCOM), field operating agencies (FOA), and direct reporting units (DRU) send one copy of their supplement to HQ AFCA/XPPD. Refer to Attachment 1 for a glossary of references, abbreviations, acronyms, and terms.

SUMMARY OF REVISIONS

This AFI supersedes Chapter 8 of Air Force Manual (AFMAN) 37-126, *Preparing Official Communications*. A (★) preceding the publication title indicates a major revision from the previous edition.

1. Purpose and Scope. This instruction lists responsibilities for users and managers of Air Force e-mail systems and provides rules for system use. E-mail is used to supplement or replace traditional mail, facsimile, telephone, and other messaging systems. This instruction applies to all uses of Air Force e-mail systems by Air Force organizations, personnel, and contractors regardless of the classification of the information transmitted or received.

2. Roles and Responsibilities.

2.1. HQ USAF/SC will establish Air Force policy for e-mail administration and use. Policies include planning, acquisition, maintenance, e-mail use, formats, e-mail address naming conventions, access, privacy, security, records management, and training responsibilities.

2.2. Air Force Functional Managers will:

2.2.1. Establish policy on the use of e-mail in their programs.

2.2.2. Determine the extent the function will use e-mail.

2.2.3. Determine the level of protection that is required for functional information sent by e-mail.

2.3. MAJCOMs, DRUs, and FOAs will:

2.3.1. Disseminate and implement Air Force e-mail policy within their organizations.

2.3.2. Identify and establish any additional or more restrictive policies for e-mail administration and use within their organizations.

2.4. Wing, Wing-Level Equivalents, and Tenant Organizations will:

2.4.1. Disseminate and implement Air Force and MAJCOM e-mail policy within their organizations.

Supersedes: AFMAN 37-126, Chapter 8, 10 February 1995. Certified by: HQ USAF/SCXX (Colonel Brian D. Miller)
OPR: HQ USAF/SCXX (Mr. Paul Armel) Pages: 17/Distribution: F

2.4.2. Identify and establish any additional or more restrictive policies for e-mail administration and use within their organizations.

2.5. Commanders will:

2.5.1. Manage the use of e-mail within their command that is consistent with Air Force and MAJCOM policy.

2.5.2. Set up initial and annual refresher training programs to make sure all e-mail users are trained on Air Force e-mail policy and appropriate use (see paragraph 12).

2.5.3. Set up procedures for internal storage and control of e-mail consistent with Air Force information security and records management policies.

2.5.4. Make sure unit out processing includes the e-mail system administrator to remove unnecessary accounts.

2.6. E-mail Administrators (typically System or Workgroup Administrators or Network Managers) will:

2.6.1. Implement and monitor compliance with Air Force e-mail policy.

2.6.2. Manage the day-to-day operations of the assigned Air Force e-mail systems and act as the primary points of contact for e-mail policy implementation.

2.6.3. Report violations of policy to appropriate authorities for further action.

2.6.4. Implement Air Force and Defense Information Systems Agency (DISA) electronic messaging registration procedures according to AFI 33-127, *Electronic Messaging Registration and Authority.*

2.6.5. Ensure the confidentiality of e-mail viewed in the performance of their duties.

2.7. E-mail Users will:

2.7.1. Comply with the Air Force e-mail policy.

2.7.2. Maintain sole responsibility for the content of their e-mail messages and ensure that messages they send meet Air Force directives regarding appropriate use of e-mail (see paragraph 3.5).

2.7.3. Make sure information received or transmitted that constitutes an Air Force record is maintained according to Air Force records management directives: AFMAN 37-123, *Management of Records* (will convert to AFMAN 33-323); AFI 37-138, *Records Disposition--Procedures and Responsibilities* (will convert to AFI 33-338), and AFMAN 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-339) (see paragraph 9 for more detailed records management guidance).

2.7.4. Make sure the account from which the e-mail message was sent is clearly identified (either in the "FROM" element of the e-mail header, the "BODY" of the message, or both). E-mail senders will not use anonymous accounts or forwarding mechanisms that purposely attempt to conceal the originator of a message unless approved by the commander for the purposes of soliciting anonymous feedback.

2.7.5. Get approval from their chain of command before subscribing to or participating in e-mail listservers and newsgroups except official Air Force internal information products. These products are managed and approved by the Headquarters Air Force News Agency, Kelly AFB, Texas. This policy recognizes that listservers are a potentially valuable information tool for e-mail users; however, the potential for abuse is high. Approve each listserver individually. Blanket approval for user participation in all listservers is not appropriate.

2.7.6. Report any suspected violations of e-mail policy to their supervisor, information protection office, or e-mail administrator.

2.7.7. Verify the authenticity of messages received if the authenticity of the message is uncertain.

3. Use. Air Force employees will use Federal Government communications systems with the understanding that such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized. Monitoring or reading another individual's e-mail messages is illegal under the Federal Wiretap Law. Under no circumstance will "monitoring" include reading individual e-mail messages without written direction by the commander or local law enforcement officials.

3.1. E-mail is official communication. You may use e-mail to transmit both formal and informal correspondence. E-mail account users bear sole responsibility for material they access and send in e-mail.

3.1.1. Use formal e-mail to replace or supplement formal Air Force formats for communications like official memorandums, messages, orders, or letters. It includes most organizational e-mail and individual e-mail that requires formal documentation.

3.1.2. Use informal e-mail to replace or supplement telephone calls, notes, or informal communication between individuals. It includes most individual e-mail and organizational e-mail that does not require formal documentation.

3.2. Transmitting official taskings. You may use e-mail systems to transmit official taskings. The sender should decide whether to send an official tasking from or to an individual or organizational e-mail address.

3.2.1. It is the sender's responsibility to make sure taskings are received by the intended receiver. Senders may request explicit acknowledgment of taskings. Some e-mail systems have features allowing users to request acknowledgments or receipts showing that a message reached the mailbox or in box of each addressee, or that an addressee opened the message.

3.2.2. It is the receiver's responsibility to validate the tasking.

3.3. Establishing organizational e-mail accounts.

3.3.1. All USAF organizations with e-mail capability will establish organizational e-mail accounts.

3.3.2. Organizational e-mail accounts will use the Air Force standard organizational abbreviations and standard Air Force office symbols as the “UserID” (see paragraph 5 for guidance).

3.3.3. Each office will designate an individual or individuals to monitor the account’s mailbox regularly to make sure messages requiring action are acted upon promptly. Each individual should have a unique identifier that the system can authenticate and provide an audit trail. When e-mail systems cannot provide a unique identifier, use administrative procedures to provide the audit trail.

3.3.4. Set up separate organizational e-mail accounts for wing commanders, vice wing commanders, senior enlisted advisors, group commanders, squadron commanders, and staff agencies. Set up other organizational accounts at the discretion of unit commanders.

3.3.5. Set up separate organizational e-mail accounts for division levels at higher headquarters, including but not limited to centers, numbered air forces, MAJCOMs, FOAs, DRUs, HQ USAF, and the Air Force Secretariat. Set up other organizational accounts as needed.

3.4. You may use individual e-mail accounts for both formal and informal communications. Make the accounts available for personnel at Air Force locations where the capability exists, and where deemed appropriate to facilitate Air Force communications unless specifically prohibited by law, policy, contract, or other binding agreement.

3.5. Acceptable and unacceptable use of Air Force e-mail.

3.5.1. Air Force e-mail systems are provided to support Air Force missions; only use e-mail systems for official, authorized, and ethical activities that are in the best interest of the Air Force. “Agency designees” (the first supervisor who is a commissioned officer or a civilian above General Schedule [GS]/General Manager [GM]-11 in the chain of command or supervision of the employee concerned) can allow limited personal use of e-mail. Limited personal use must conform with theater commander-in-chief (CINC) and MAJCOM policies.

3.5.1.1. Official use includes emergency communications and communications that the Department of Defense (DoD) component determines are necessary in the best interest of the Federal Government. Official use includes, when approved by theater commanders , and in the interest of morale and welfare, communications by military members and other DoD employees who are deployed for extended periods away from home on official DoD business.

3.5.1.2. Authorized personal use includes brief communications made by DoD employees while traveling on US Government business to notify family members of official transportation or schedule changes. They also include personal communications from the DoD employee’s usual workplace that are most reasonably made while at the workplace (such as checking in with spouse or minor children; scheduling doctor, automobile, or home repair appointments; brief internet searches; or e-mailing directions to visiting relatives), when the “agency designee” permits categories of communications, determining that such communication:

3.5.1.2.1. Does not adversely affect the performance of official duties by the DoD employee or the DoD employee’s organization.

3.5.1.2.2. Is of reasonable duration and frequency, and whenever possible, made during the DoD employee’s personal time, such as after-duty hours or lunch periods.

3.5.1.2.3. Serves a legitimate public interest (such as keeping DoD employees at their desks rather than requiring the use of commercial systems, educating the DoD employee on the use of the communications system, improving the morale of DoD employees stationed for extended periods away from home, enhancing the professional skills of the DoD employee, or job-searching in response to Federal Government downsizing).

3.5.1.2.4. Does not put Federal Government communications systems to use that would reflect adversely on DoD or the DoD component (for example, pornography, chain letters, unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use, violations of statute or regulation, inappropriately handled classified information, or other uses that are incompatible with public service).

3.5.1.2.5. Does not overburden the communications system (such as with large broadcasts or group mailings).

3.5.1.2.6. Creates no significant additional cost to DoD or the DoD component.

3.5.2. The basic standards for using e-mail are common sense, common decency, and civility applied to the electronic communications environment. This includes following traditional military protocols and courtesies.

3.5.3. Unacceptable use of Air Force e-mail systems include, but are not limited to, the following:

3.5.3.1. Attaching to e-mail, or otherwise distributing copyrighted materials by e-mail without first getting consent from the copyright owner. Failure to maintain consent may violate federal copyright infringement laws that could subject the individual to civil liability or criminal prosecution.

3.5.3.2. Sending or receiving e-mail for commercial or personal financial gain using Air Force systems.

3.5.3.3. Intentionally or unlawfully misrepresenting your identity or affiliation in e-mail communications.

3.5.3.4. Sending harassing, intimidating, abusive, or offensive material to or about others that violates Air Force standards of behavior. This includes, but is not limited to, humor considered in poor taste or offensive, political or religious lobbying, and pornographic material.

3.5.3.5. Using someone else’s identity (userID) and password without proper authority.

3.5.3.6. Causing congestion on the network by such things as the propagation of chain letters, broadcasting inappropriate messages to lists or individuals, or excessive use of the data storage space on the e-mail post server.

3.6. Subscription Services. Internet e-mail access grants users the ability to subscribe to a variety of e-mail newsgroups, listservers, and other sources of information. These services may include professional newsgroups sponsored by Air Force agencies and other newsgroups sponsored by agencies outside the Air Force, including the DoD, other federal agencies, educational institutions, and commercial activities. These services are a potentially valuable information tool for some e-mail users; however, the potential for abuse is high.

3.6.1. Commanders may authorize USAF personnel to subscribe to electronic mail groups if participation in those discussions is an essential part of the member's duty. These e-mail groups may include, but are not limited to, process action teams, working groups, or permanent committees.

3.6.2. Users must get approval from their chain of command before subscribing to or participating in e-mail listservers that are not official Air Force internal information products or required as part of their official duties. Recommended approval levels are unit commanders at base level and division chiefs at headquarters. Users who participate in external newsgroups or listservers using government equipment must clearly state in all messages that the opinions expressed are those of the individual and do not represent an official position of the United States Air Force.

3.6.3. Participation in newsgroups or listservers whose content is contrary to the standards set by the *Joint Ethics Regulation* (that is, obscene or offensive) is prohibited. Commanders may direct e-mail administrators to set up permanent blocks on specific newsgroup or listserver addressees that prevent subscription to such services.

3.6.4. Users are responsible for protecting Air Force information, which includes both sensitive unclassified and classified.

3.7. Users are responsible for proper coordination and staffing of e-mail in accordance with local directives.

3.8. E-mail is subject to the requirements of the *Freedom of Information Act*and the *Privacy Act of 1974*.

4. Formats.

4.1. Organizational e-mail includes official communications such as memoranda (letters), notes, messages, reports, and so forth, and will follow specific formats found in this instruction and AFMAN 37-126.

4.1.1. Senders will include a formal signature block on all organizational e-mail. For example:

FRANCIS X. MCGOVERN, Lt Col, USAF Chief, Information Policy

Policy and Strategy Division Directorate of Plans, Policy, and Resources DCS/Communications and Information

4.2. Individual e-mail typically uses a less formal writing style but is still considered official when the sender is acting in an authorized capacity.

5. Naming Conventions.

5.1. Air Force e-mail addresses are composed of the following two elements in the following form: [UserID]@[domain name]. Domain names will follow the formats specified in AFMAN 33-128, *Electronic Messaging Registration.*

5.2. Organizational e-mail accounts will use the standard organizational abbreviation from Air Force Directory (AFDIR) 37-135, *Air Force Address Directory* (will convert to AFDIR 33-335) and standard Air Force office symbols in AFMAN 37-127, *Air Force Standard Office Symbols* (will convert to AFMAN 33-327), as the UserID.

5.2.1. UserIDs for units at wing, group, and squadron level will consist of the standard organizational abbreviation and standard Air Force office symbols separated by a period. For example: 10WG.CC, 10LG.CC. You may add additional information between the two as needed for units like detachments and operating locations: For example: 10WG.DET1.CC.

5.2.2. UserIDs for higher headquarters will consist of the headquarters standard organizational abbreviation and standard Air Force office symbols separated by a period: For example: USAF.SCXX, SAF.AAD.

5.3. For individual e-mail accounts, base the UserID element of the address on the last name followed by first name of the user. For example: armel.paul. Add middle initials or numbers as needed to specifically identify users with similar names within domains: For example: smith.jane2. For systems limited to eight characters, use the last name followed by initial of first name and number if required. For example: smithj or smithj2. For last names exceeding eight letters, use the first seven letters of the last name followed by the initial of the first name or number. For example: burkhar2.

6. Authentication.

6.1. Take special care to prove the identity of a person or organization initiating an electronic transaction. To authenticate an e-mail message, you must prove its origin. Authentication does not necessarily require a digital signature. Under normal use, you may consider e-mail authentic because a log-on password is used to gain access to the mail system and send the message. However, you can make full authentication of normal e-mail conditional upon the recipient contacting the sender to confirm the transmission of the message.

6.2. The next level of authentication above mail system security involves the use of digital signatures.

6.2.1. A digital signature shows that the person who signed the document had access to the proper key and the password for the key indicated by the signature, and that the document was not modified since it was signed.

6.2.2. Proper authentication of a digital signature implies that the message was originated by the sender and that the transaction received was not modified in transit.

7. Staffing. It is permissible to use e-mail for staffing depending on local conditions and operating procedures. Local commanders should set policy regarding the use of e-mail for staffing information or action packages. When e-mail is used for staffing, use organizational accounts when sending material to offices for coordination or action. Using e-mail for coordination and staffing increases efficiency when properly managed.

8. Professional Courtesies. Air Force personnel follow certain conventions when communicating via memoranda or telephone. Use these accepted conventions to compose and disseminate information via e-mail.

8.1. The following represent generally accepted practices for electronic communications (sometimes referred to as “network etiquette” or “netiquette”):

8.1.1. Lead your message with the most important information. Make your main point in the first paragraph.

8.1.2. Follow the chain of command when sending messages up the line as you would using any other medium. Send courtesy copies as necessary.

8.1.3. Delete outdated or unwanted incoming and outgoing messages after following records management guidance provided in paragraph 9.

8.1.4. Remember the basic elements of effective writing: clarity, brevity, and courtesy.

8.1.5. Focus on one subject per message and always include a pertinent subject title for the message; that way the user can locate the message quickly.

8.1.6. Include your signature block at the bottom of e-mail messages when needed to ensure all recipients can identify the originator.

8.1.7. Capitalize words only to highlight an important point or to distinguish a title or heading. You can also use *asterisks* surrounding a word to make a stronger point. Capitalizing whole words that are not titles is generally considered SHOUTING. Do not SHOUT unless you need to emphasize a particular point.

8.1.8. Be professional and careful whenever you write about others. Understand that e-mail is easily forwarded; and that messages that are intended to be private or personal may not remain so. Material sent via e-mail is not confidential, and is subject to monitoring and retransmittal.

8.1.9. Use a tone of address that is appropriate to the recipient.

8.1.10. Cite all quotations, references, and sources.

8.1.11. Watch the use of unprofessional language and limit the use of sarcasm and humor. Without face-to-face communications, the recipient may view your “joke” as criticism.

8.1.12. Use acronyms to abbreviate when feasible. However, senders should recognize that messages filled with acronyms are confusing and annoying to the reader. Use acronyms that are of a common-use-nature, and understood by the intended audience. “Spell out” acronyms in the first instance of use.

8.1.13. Know and consider the limitations of your system. For example, sending large files such as digital images to a large number of recipients will delay other traffic and may overload the system causing failure.

8.1.14. Edit messages for spelling and grammatical errors.

8.1.15. Use caution when sending an e-mail message to “all” and other type address groups. Imprudent use of such address groups clogs e-mail accounts and often clutters in-boxes.

8.2. Listservers, Mailing Lists, and Discussion Groups.

8.2.1. When you join a list, monitor the messages for a few days to get a feel for what common questions are asked, and what topics are deemed off-limits. This is commonly referred to as “lurking.”

8.2.2. See if there are any frequently asked questions (FAQ) for a group that you are interested in joining. Other members get annoyed when they see the same questions every few weeks.

8.2.3. Keep in mind that some discussion lists or Usenet groups have members from many countries. Do not assume that they will understand a reference to TV, movies, pop culture, or current events in your country. If you must use the reference, please explain it.

8.2.4. Keep your questions and comments relevant to the focus of the discussion group. Otherwise, you are subject to receiving a high volume of nuisance e-mails (flamed) as the group expresses it displeasure with you. This is likely to cause problems not only to you, but also affect system operations for all other users.

8.2.5. If another person posts a comment or question that is off the subject, do not reply to the list or keep the off-subject conversation going publicly.

8.2.6. When an extended absence will not allow access to your e-mail account, unsubscribe or suspend mail from any mailing lists or listservers. This will alleviate large backlogs of received messages filling server storage resources.

8.2.7. When quoting another person, edit out what is not directly applicable to your reply. Do not let your mailing or Usenet software automatically quote the entire body of messages you are replying to when it is not necessary. Take the time to edit any quotations down to the minimum necessary to provide context for your reply.

8.2.8. Use discretion when forwarding a long mail message to group addressees or distribution lists. It is preferable to reference the source of a document and provide instructions on how to get a copy. If you must post a long message, warn the readers with a statement at the top of the mail message or subject line. Example: “Warning: Long Message.”

8.2.9. When replying to a message posted to a discussion group, check the address to make sure it is going to the intended location (person or group). It can be very embarrassing to reply incorrectly and post a personal message to an entire discussion group that was intended for only one individual.

8.2.10. The use of automatic response (for example, “I’m out of the office”) messages is discouraged because listservers and mail reflectors react poorly to these types of messages.

9. Records Management Standards.

9.1. Federal Records Act . The *Federal Records Act* requires the Air Force to identify and preserve records including records created or received on e-mail systems.

9.2. Determining Record Status. E-mail messages are records when they meet both of the following conditions:

9.2.1. They are made or received by an agency of the United States Government under federal law, or in connection with the transaction of agency business.

9.2.2. They are preserved or are appropriate for preservation as evidence of agency organization and activities, or because of the value of the information they contain.

9.3. Working Files and Similar Materials. Maintain working files, such as preliminary drafts and “rough” notes, and other similar materials for adequate and proper documentation if:

9.3.1. They were circulated or made available to employees, other than the creator, for official purposes such as approval, comment, action, recommendation, follow-up, or to communicate with agency staff about agency business; and

9.3.2. They contain unique information, such as substantive annotations or comments included therein, that adds to a proper understanding of the agency’s formulation and execution of basic policies, decisions, actions, or responsibilities.

9.4. Record Status of Copies. The determination whether a particular document is a record does not depend on whether it contains unique information. Multiple copies of the same document and documents containing duplicative information, including messages created or received on electronic mail systems, may each have record status depending on how they are used to transact agency business.

9.5. E-mail messages containing information that serves as adequate and proper documentation of the organization, functions, policies, decisions, procedures, and transactions are records.

9.5.1. E-mail records, like federal records in any other media, must be systematically managed.

9.5.1.1. Preserve the content, context, and structure of records in a useable format for their authorized retention period. A complete e-mail record will include the message itself; any attachments, such as word processing and other electronic documents transmitted with the message; and transmission data, including, but not limited to, the names of sender and addressees and date and time the message was sent.

9.5.1.2. Make them easily accessible by individuals who have a business need for information in the system.

9.5.1.3. Arrange them as groups of related records by classification according to the nature of the business purposes the records serve and as shown on the office file plan.

9.5.1.4. Protect records from unauthorized or unintentional disclosure or destruction (see paragraph 10).

9.5.1.5. Destroy in accordance with AFMAN 37-139.

9.5.1.6. Preserve e-mail system information that identifies users by codes or nicknames, or identifies addressees by the name of a distribution list, to ensure identification of the sender and addressees of messages that are records.

9.5.1.7. Preserve receipts or acknowledgments, when these options are used, that show when a message reached the mailbox or inbox of each addressee or that an addressee opened a message with the official e-mail record (see paragraph 3.2.1).

9.5.1.8. Make sure federal records sent or received on e-mail systems outside organizational control are preserved, and that reasonable steps are taken to capture available transmission and receipt data needed by the agency for record-keeping purposes.

9.5.1.9. Store record copies of e-mail messages in systems designed as record-keeping systems.

9.5.1.10. When an e-mail record is retained in a record-keeping system, the e-mail message may be deleted from the e-mail system.

9.5.2. Get approval for any electronic system used for record-keeping purposes from the local records manager.

9.6. Some e-mail systems provide calendars and task lists for users. These calendars and task lists may meet the definition of a federal record.

9.6.1. Calendars, appointment books, schedules, logs, diaries, and other records documenting meetings, appointments, telephone calls, trips, visits, and other activities by federal employees serving in an official capacity, created and maintained in hard copy or electronic form, EXCLUDING materials that are personal, that contain substantive information relating to official activities, the substance of which is not incorporated into official files, meet the definition of federal records and are managedin accordance with the provisions of AFMAN 37-139.

10. Security.

10.1. The internet is an unsecured network. Information packets traveling across the internet are routed through many nodes to travel from origin to destination. Interception of the information can occur at any point along the way. To prevent unauthorized disclosure of information, you must implement sufficient access and security controls to protect the information. Determine the level of security measures required by the sensitivity of the information.

10.2. It is DoD policy that we:

10.2.1. Safeguard classified and sensitive unclassified information at all times. Apply safeguards so that such information is accessed only by authorized persons, is used only for its intended purpose, retains its content integrity, and is marked properly as required by Office of Management and Budget (OMB)/Information Security Oversight Office (ISOO) Directive No. 1, *Classified National Security Information*.

10.2.2. Safeguard all unclassified information against tampering, loss, and destruction. This is necessary to protect the DoD investment in obtaining and using information and to prevent fraud, waste, and abuse.

10.2.3. Safeguard information and e-mail system resources (against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons) through the continuous employment of safeguards consisting of administrative, procedural, physical and/or environmental, personnel, communications, emanations, operations, information, and computer security.

10.2.4. Make sure the mix of safeguards selected for e-mail systems that process classified or sensitive unclassified information meets the minimum requirements as set forth in DoD Directive (DoDD) 5200.28, *Security Requirements for Automated Information Systems (AISs)*, May 21, 1988, Enclosure 3. Meet these minimum requirements through automated and manual means in a cost-effective and integrated manner. Perform analysis using DoDD 5200.28 Enclosure 4 to identify any additional requirements over and above the set of minimum requirements.

10.2.5. DoD military, civilian, consultants, and contractor personnel using unclassified automated information systems must have, at a minimum, a National Agency Check/Entrance National Agency Check in accordance with DoD 5200.2-R, *Personnel Security Program*, January 1987. Those personnel requiring access to classified systems are subject to the appropriate investigative scope.

10.3. Classified E-mail.

10.3.1. Network and e-mail administrators must possess a security clearance equal to the highest security of the network they administer.

10.3.2. When transmitting classified information via e-mail, take special care to transmit only that level of classified information for which the system is authorized (see Attachments 3 and 4).

10.3.3. Mark classified e-mail messages using internal portion markings prescribed in OMB/ISOO Directive No. 1. Mark all classified e-mail messages to reflect the highest classification of the information contained in the transmission. Should the message contain an attachment, the overall classification marking on the e-mail message must reflect the highest classification of information contained within the entire e-mail transmission (see Attachments 2, 3, and 4). Mark all paragraphs and subparagraphs with their classification in the same manner as normal correspondence.

10.3.4. Classified e-mail will contain declassification instructions. The end of the message text must include declassification or downgrading instructions. See AFI 31-401, *Managing the Information Security Program*, for additional guidance.

10.3.5. Use electronic delivery receipts when transmitting classified information off the installation or to non-Air Force activities.

10.3.6. Confirm a person's clearance by completing one of the following:

10.3.6.1. Checking the person's access on the Automated Security Clearance Approval System (ASCAS) roster (this only applies to Air Force employees).

10.3.6.2. Checking with the employee's security manager, supervisor, or commander.

10.3.6.3. Checking the clearance level on a person's temporary duty (TDY) orders.

10.3.6.4. Receiving a visit request from the visitor's security manager or supervisor. See AFI 31-401, paragraph 7.4, for further guidance.

10.3.7. Destroying Classified E-mail.

10.3.7.1. Holders destroy classified e-mail that is no longer required. If the classified e-mail is the official record, destroy only after the retention period in AFMAN 37-139 has expired. See Air Force Systems Security Instruction (AFSSI) 5100, *The Air Force Computer Security (COMPUSEC) Program*, and AFSSI 5102, *Computer Security (COMPUSEC) for Operational Systems* (both AFSSIs will convert to AFI 33-202) for further guidance. For paper e-mail products, consult AFI 31-401.

10.3.7.2. Top Secret control officers (TSCO) use AF Form 143, **Top Secret Register Page**, or another approved form (for example, AF Form 310, **Document Receipt and Destruction Certificate**) to record destruction of Top Secret e-mail.

10.3.7.2.1. Attach the form to the Top Secret register page.

10.3.7.3. When you must keep a record of destroyed Secret and Confidential materials, holders choose from:

- AF Form 310.
- AF Form 1565, **Entry, Receipt, and Destruction Certificate** (for document page changes).

10.3.7.4. Base network control center (BNCC) personnel destroy classified residue by-products as they would classified waste. Additional guidance for purging or destroying electronic media is found in AFSSI 5020, *Remanence Security* (will convert to AFMAN 33-224).

10.4. Unclassified E-mail.

10.4.1. Special Handling Requirements. Do not transmit unclassified information that requires special handling (for example, encrypt for transmission only [EFTO]), on or to systems not approved for that purpose.

10.4.1.1. "PERSONAL FOR" Messages. When using organizational e-mail boxes, general or flag officers and civilians of equivalent rank may originate "PERSONAL FOR" e-mail messages. The caveat "PERSONAL FOR" is established by Allied Communications Publication (ACP) 121, (C) *DCS Operating Procedures* (U), and means you must protect the privacy of the message. Deliver "PERSONAL FOR" messages to the individual named or designated representative's personal e-mail address. Use the caveat "PERSONAL FOR (name)" or "PERSONAL FOR (name) FROM (name)" in the e-mail subject line.

10.4.2. You may transmit unclassified information on classified networks unless specifically prohibited by the network operating instructions. The guidelines listed below apply to all unclassified e-mail sent across any network including those cleared for classified material (see Attachment 5).

10.5. Sensitive Unclassified Information.

10.5.1. Operations Security (OPSEC). Adversaries of the United States have very well developed methods of collecting valuable information from and about Air Force activities and operations to thwart or forestall the effectiveness of United States intentions. To deny or control "critical information," the Air Force must plan and execute OPSEC measures. OPSEC is our first line of defense against these intelligence collection efforts. If successful, adversaries are then able to improve their own plans, operations, weapon systems, and defense systems by limiting, evading, or defeating Air Force warfighting capabilities. Users of e-mail systems must stay constantly aware of communications systems vulnerabilities and the need to safeguard "critical information," OPSEC indicators, and sources of such information. As a minimum, you must encrypt "critical information," OPSEC indicators, and sources of such information before transmission across the internet. Keep in mind that some discussion lists and Usenet groups have members from many foreign countries and discussions in these groups may lead to inadvertent disclosure of sensitive information.

10.5.1.1. Identification of Critical Information. Critical information is information about friendly (US, allied, and coalition) activities, intentions, capabilities, or limitations that an adversary needs to gain a military, political, diplomatic, or technological advantage. Such information, if released to an adversary prematurely, may prevent or forestall mission accomplishment, reduce mission effectiveness, or cause an unacceptable loss of lives and damage to friendly resources. Critical information usually involves only a few key items of information about friendly activities, intentions, and so forth, that, if known by the adversary, could drastically degrade mission effectiveness (for example, "time over target"). You can also derive critical information from bits and pieces of related information (indicators) that are almost always available to the trained eye.

10.5.2. Privacy Act Information. The right to privacy is a personal and fundamental right protected by the *Constitution of the United States*. The *Privacy Act of 1974* provides safeguards protecting individuals against an invasion of personal privacy. As such, the privacy of an individual is directly affected by the electronic collection, maintenance, use, and dissemination of personal information. To protect the privacy of individuals when sending Privacy Act information across the internet, use an appropriate level of protection to prevent unintentional or unauthorized disclosure. Follow the procedures in AFI 37-132, *Air Force Privacy Act Program* (will convert to AFI 33-332), for safeguarding Privacy Act information. The following items of information are examples of information normally protected from disclosure:

- Marital status.
- Number or sex of dependents.
- Gross salary of military personnel.
- Civilian educational degrees and major areas of study.
- School and year of graduation.
- Home of record.
- Home address or phone number.
- Age or date of birth.
- Present or future assignments for overseas or for routinely deployable or sensitive units.
- Office, unit address, and duty phone for overseas or for routinely deployable or sensitive units.

10.5.2.1. Social Security account numbers (SSAN) are personal and unique for each individual and must be protected as For Official Use Only (FOUO)(see AFI 37-131, *Freedom of Information Act Program* [will convert to AFI 33-331]). When sending SSANs across the internet, use an appropriate level of protection to prevent unintentional or unauthorized disclosure.

10.5.2.2. There are exceptions in the *Privacy Act* that allow disclosure of personal information without consent of the subject. The most widely used exception is to those persons within the agency who have an official need to know. Do not disclose personal information to large personal or organizational e-mail groups.

10.5.3. Freedom of Information Act (FOIA). The Air Force discloses its records in its possession and control to the public, except those records exempt under FOIA which, if released, would cause identifiable harm. The following categories of information are normally exempt from routine disclosure and you must protect them from unintentional or unauthorized disclosure:

- Classified information.
- Internal personnel rules and practices.
- Information specifically exempted from disclosure by other statutes.
- Confidential commercial information.
- Inter- or Intra-agency records that are deliberative or predecisional in nature.
- Information whose disclosure would constitute an invasion of privacy.
- Investigative record or information gathered for law enforcement purposes.
- Records of an agency that regulates or supervises financial institutions.
- Records with geological and geophysical information and data, including maps concerning wells.

10.5.3.1. Do not send information normally exempt under FOIA across the internet without an appropriate level of protection to prevent unintentional or unauthorized disclosure. Follow the procedures in AFI 37-131.

10.5.3.2. Refer to AFI 37-131 for additional guidance.

10.5.4. Protection of E-mail Addresses. To reduce the risk of attack on Air Force e-mail systems, do not indiscriminately release e-mail addresses. Lists of overseas, sensitive, or routinely deployable unit individual or organizational e-mail addresses are exempt from disclosure under the FOIA.

10.6. Physical Security. The e-mail system administrator must set up procedures defining the control, security, access, and upkeep of all e-mail storage media.

10.6.1. Off-site Storage. Keep selected archived e-mail files required for system reconstitution after catastrophic system failure in a secure area, physically separated from the network control center/e-mail server. Select the off-site storage location based on its proximity to the network control center/e-mail server, the temperature and humidity, and the physical security of the building.

Place a priority schedule for recreating files at the off-site storage location.

10.7. E-mail Access. Access by foreign nationals to US Government-owned or US Government- managed automated information systems is authorized only by the DoD component head, and must remain consistent with the DoD, the Department of State, and the Director of Central Intelligence Agency policies. Reference DoDD 5200.28.

11. Information Collections and Reports (ICR).

11.1. You can use e-mail messages to collect status, summary, or statistical information from other organizations. This type of information collection is considered an internal reporting requirement and must reference a report control symbol (RCS). Refer to AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and InterAgency Air Force Information Collections* (will convert to AFI 33-324), for the proper procedures for applying for an RCS number before soliciting information through e-mail.

11.2. You can also use e-mail to solicit information from the public (for example, a questionnaire, customer survey, and so forth). This type of information collection must be approved and licensed by the OMB. Refer to AFI 37-124 for further guidance.

12. Training.

12.1. Commanders must make sure e-mail users within their command are educated and trained on the appropriate use of e-mail. Training will include:

12.1.1. Security.

12.1.1.1. Information security.

12.1.1.2. Operational security.

12.1.1.3. System security.

12.1.2. Professional Courtesies.

12.1.3. Local Operating Procedures.

12.1.4. User Responsibilities.

12.1.5. Records Management Requirements.

12.1.6. Authorized Use.
12.1.7. Unauthorized Use.
12.1.8. Systems Operations and Capabilities.
12.1.9. Privacy Act
12.1.10. Public Release of Information and FOIA.

WILLIAM J. DONAHUE, Lt General, USAF
DCS/Communications and Information

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

References

ACP 121, (C) *DCS Operating Procedures (U)*
AFDIR 37-135, *Air Force Address Directory* **(will convert to AFDIR 33-335)**
AFI 31-401, *Managing the Information Security Program*
AFI 33-127, *Electronic Messaging Registration and Authority*
AFI 35-205, *Air Force Security and Policy Review Program*
AFI 37-131, *Freedom of Information Act Program* **(will convert to AFI 33-331)**
AFI 37-132, *Air Force Privacy Act Program* **(will convert to AFI 33-332)**
AFI 37-138, *Records Disposition--Procedures and Responsibilities* **(will convert to AFI 33-338)**
AFMAN 33-128, *Electronic Messaging Registration*
AFMAN 37-123, *Management of Records* **(will convert to AFMAN 33-323)**
AFMAN 37-126, *Preparing Official Communications* **(will convert to AFMAN 33-326)**
AFMAN 37-127, *Air Force Standard Office Symbols* **(will convert to AFMAN 33-327)**
AFMAN 37-139, *Records Disposition Schedule* **(will convert to AFMAN 33-339)**
AFPD 31-4, *Physical Security*
AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*
AFSSI 5020, *Remanence Security* **(will convert to AFMAN 33-224)**
AFSSI 5100, *The Air Force Security (COMPUSEC) Program* **(will convert to AFI 33-202)**
AFSSI 5102, *Computer Security (COMPUSEC) for Operational Systems* **(will convert to AFI 33-202)**
DoDD 5200.28, *Security Requirements for Automated Information Systems (AISs)*, May 21, 1988
DoD 5200.1-PH, *A Guide to Marking Classified Documents*, November 1982
DoD 5200.2-R, *Personnel Security Program*, January 1987
OMB/ISOO Directive No. 1, *Classified National Security Information*

Abbreviations and Acronyms

AFCA−Air Force Communications Agency
AFDIR−Air Force Directory
AFI−Air Force Instruction
AFMAN−Air Force Manual
AFPD−Air Force Policy Directive
AFSSI−Air Force Systems Security Instruction
ASCAS−Automated Security Clearance Approval System
BNCC−Base Network Control Center
CINC−Commander-in-Chief
CNWDI−Critical Nuclear Weapon Design Information
CSO−Communications-Information Systems Officer
DISA−Defense Information Systems Agency
DoD−Department of Defense
DoDD−Department of Defense Directive
DRU−Direct Reporting Unit
EFTO−Encrypt for Transmission Only
E-mail−Electronic Mail
FAQ−Frequently Asked Questions
FOA−Field Operating Agency
FOIA−Freedom of Information Act
FOUO−For Official Use Only
GM−General Manager (civilian grade system)
GS−General Schedule (civilian grade system)
ICR−Information Collections and Reports
ISOO−Information Security Oversight Office
LIMDIS−Limited Distribution
MAJCOM−Major Command
OMB−Office of Management and Budget

OPSEC−Operations Security
RCS−Report Control Symbol
SSAN−Social Security Account Number
TCP/IP−Transmission Control Protocol/Internet Protocol
TDY−Temporary Duty
TSCO−Top Secret Control Officer
UCMJ−Uniform Code of Military Justice
USAF−United States Air Force

Terms

Agency Designee—The first supervisor who is a commissioned officer or a civilian above GS/GM-11 in the chain of command or supervision of the employee concerned.

Authorized E-mail—E-mail sent or received on an Air Force e-mail system. This includes e-mail directly related to:

- Accomplishment of the mission or function of organization.
- Individuals' professional development.
- Personal e-mail authorized by the "agency designee."
- Commanders and supervisors may authorize any use that is directed by the *Uniform Code of Military Justice (UCMJ)* and *Joint Ethics Regulation*, and does not interfere with mission performance.

Communications-Information Systems Officer (CSO)—The term CSO identifies the supporting CSO at all levels. At base-level, this is the commander of the communications unit responsible for carrying out base communications and information systems responsibilities. At MAJCOM and other activities, it is the person designated by the Commander as responsible for overall management of communications-information systems budgeted and funded by the MAJCOM or activity. The CSO function uses the office symbol "SC" which is expanded to three and four digits to identify specific functional areas. CSOs are the accountable officers for all automated data processing equipment in their inventory.

Frequently Asked Questions (FAQ)—A document that is available to newsgroup or listserver subscribers that outlines those questions and their answers that are commonly asked by members of the newsgroup or listserver. It is designed as a resource for new users so that they do not have to ask repetitive questions to other subscribers.

Individual E-mail Account—An e-mail account created for and accessed by a single individual only.

Individual Message—This type of message includes routine communications between individual DoD personnel within administrative channels, both internal and external to the individual organizational element. Informational messages and those requiring only a basic transport service (the electronic analogue of the telephone call) are treated as a part of this class.

Information Protection Office—Formerly "C4 Systems Security Office (CSSO)".

Internet—An informal collection of government, military, commercial, and educational computer networks using the transmission control protocol/internet protocol (TCP/IP) to transmit information. The global collection of interconnected local, mid-level and wide-area networks that use IP as the network layer protocol.

Listserver—An electronic mailing list of individuals interested in a specific common topic. Individuals subscribe to listservers by sending an e-mail message asking to be placed on the "list." Once added to the list, members will receive all messages sent to the "list" and may post their own messages. Messages posted to the "list" are sent to all other subscribers.

Netiquette—Commonly accepted practices or conventions used when communicating using electronic means.

Newsgroup—Internet resources by which individuals interested in a particular topic may read and post messages that are accessed, read, and responded to by other internet users. Newsgroups are moderated (where messages are screened for appropriateness before posting by individuals in charge of the newsgroup), or unmoderated (where all messages are posted, regardless of content).

Naming Conventions—A method of uniquely identifying an e-mail address on a network.

Nonrecord Information materials that are not part of the legal definition of a record. Includes extra copies of documents kept only for convenience of reference, stocks of publications and of processed documents, and library or museum materials intended solely for reference or exhibition.

Official Record—Recorded information, regardless of media, maintained by an agency to comply with its legal obligations or created as a result of its transactions of public business. Excluded as records are library and museum materials, extra copies of documents preserved for convenience or references, stocks of publications, and blank forms.

Organizational E-mail Account—An e-mail account used to receive and send organizational messages. Send official correspondence that tasks an organization to an organizational account.

Organizational Message—This type of message includes command and control traffic and messages exchanged between organizational elements. These messages require release by the sending organization and distribution determination by the receiving organization. Due to their official and sometimes critical nature, such messages impose operational requirements on the communications systems for such capabilities as non-routine precedence, guaranteed timely delivery, high availability and reliability, and a specified level or survivability.

Records—All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by any agency of the US Government under federal laws, or with the transaction of public business, and preserved or appropriate for preservation by an agency, or its legitimate successor, as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and processed documents are not included.

Record-keeping System—A record-keeping system made up of a set of policies, procedures, and equipment that are used to organize and identify files or documents to speed up their retrieval, use, and disposition.

Registered Objects—Refers to the globally unique messaging components that are registered with the Air Force Registration Authority or the Sub-Registration Authorities. These messaging components include directory names, electronic messaging addresses, security certificates and routing information.

MARKING CLASSIFIED ELECTRONIC MAIL MESSAGES

A2.1. Classified Information. Mark classified e-mail messages to show the level of classification of the information contained in or revealed by it.

A2.1.1. Mark all e-mail messages on classified networks by entering the appropriate classification in parenthesis by using these symbols: “(S)” for Secret, “(C)” for Confidential, and “(U)” for Unclassified, as the first marking in the “Subject” box of the message template. Following the subject, place the appropriate symbol indicating the appropriate classification of the subject itself. Do not mark messages on unclassified network (see Attachment 5).

A2.1.2. Place the appropriate classification of the e-mail transmission in all uppercase letters as the first line of the e-mail message text. Include no other information on this line.

A2.1.3. Begin the text of the message on the third line (that is, leave one blank line between the classification marking and the beginning of the e-mail message text).

A2.1.4. Use abbreviated classification symbol at the beginning of all paragraphs and subparagraphs.

A2.1.5. Place the appropriate classification of the e-mail transmission in all uppercase letters as the last line of the e-mail text. Include no other information on this line.

A2.1.6. Indicate the security classification of any attachments by placing the abbreviated classification symbol in parentheses before the attachment icon. If the e-mail message is unclassified without the attachments, then add this mandatory line: “THIS MESSAGE IS UNCLASSIFIED WHEN SEPARATED FROM ATTACHMENT.”

A2.1.7. Place Critical Nuclear Weapon Design Information (CNWDI), Cryptographic, Restricted Data, or other designators indicating special handling in the text following the security classification. Place markings for RESTRICTED DATA-ATOMIC ENERGY ACT 1954, and FORMERLY RESTRICTED DATA ATOMIC ENERGY ACT on the message as shown in DoD Pamphlet 5200.1-PH, *Guide to Marking Classified Documents*, November 1982; AFPD 31-4, *Information Security*; and AFI 31-401, *Managing the Information Security Program*.

A2.1.8. LIMDIS (Limited Distribution) designates classified messages that must have limited distribution and special handling and must be delivered only to organizational mailboxes. Type “LIMDIS” on the first page of LIMDIS-designated e-mail messages when processing.

A2.2. Reply and Forward Actions:

A2.2.1. Reply and forward actions carry the highest classification of any information contained within the appended e-mail transmissions.

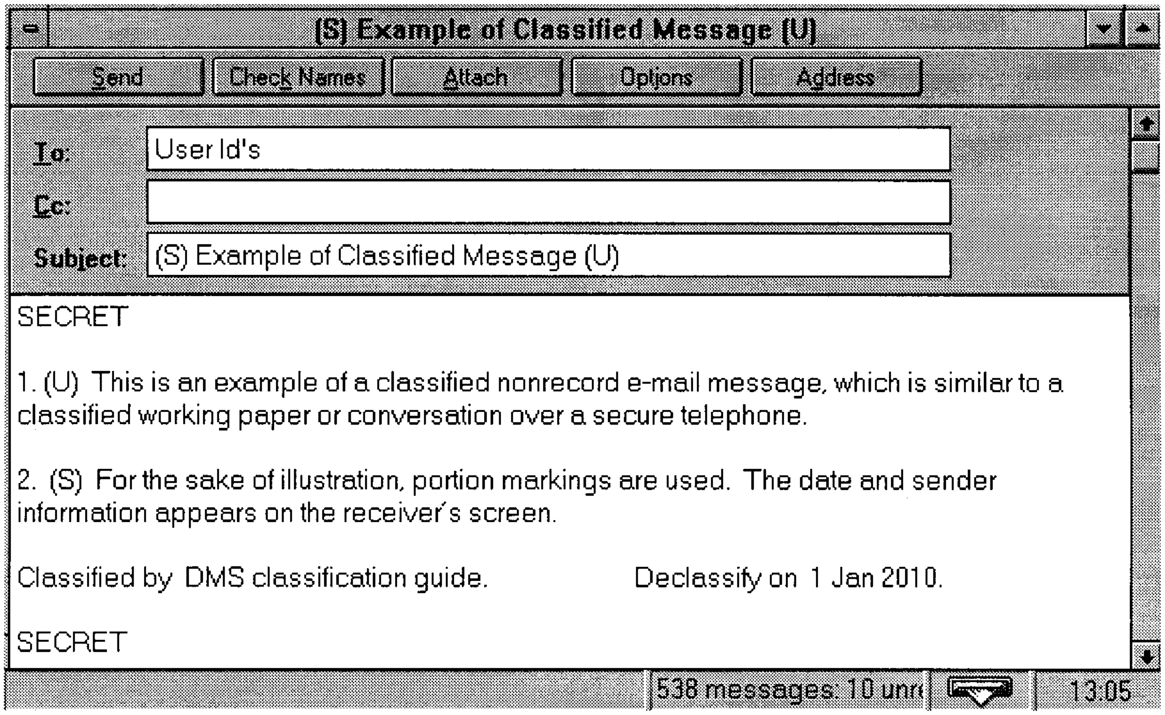
A2.2.2. Text markings included in a “Reply/Forward” will follow instructions listed above.

A2.2.3. If comments included in a “Reply/Forward” change the classification level of the e-mail transmission, then change the classification symbol of the “Subject” box and message text markings accordingly.

TRANSMITTING CLASSIFIED MESSAGES AND ATTACHMENTS

NOTE: Figure A3.1 is unclassified; security markings are for instructional purposes only.

Figure A3.1. Example of Classified E-mail Message.



To: User Id's

Cc:

Subject: (S) Example of Classified Message (U)

SECRET

1. (U) This is an example of a classified nonrecord e-mail message, which is similar to a classified working paper or conversation over a secure telephone.

2. (S) For the sake of illustration, portion markings are used. The date and sender information appears on the receiver's screen.

Classified by DMS classification guide. Declassify on 1 Jan 2010.

SECRET

NOTES:

1. Subject Line, First Entry: Appropriate classification symbol for the overall classification of e-mail transmission.

2. Subject classification symbol (classified message).

3. Text Box, First Line: Overall classification of e-mail message and attachments.

4. One blank line between classification and message text.

5. Paragraph classification symbols (classified message).

6. Attachment classification symbol.

7. Caveat for classification when e-mail message is separated from the attachment.

8. One blank line between text and classification.

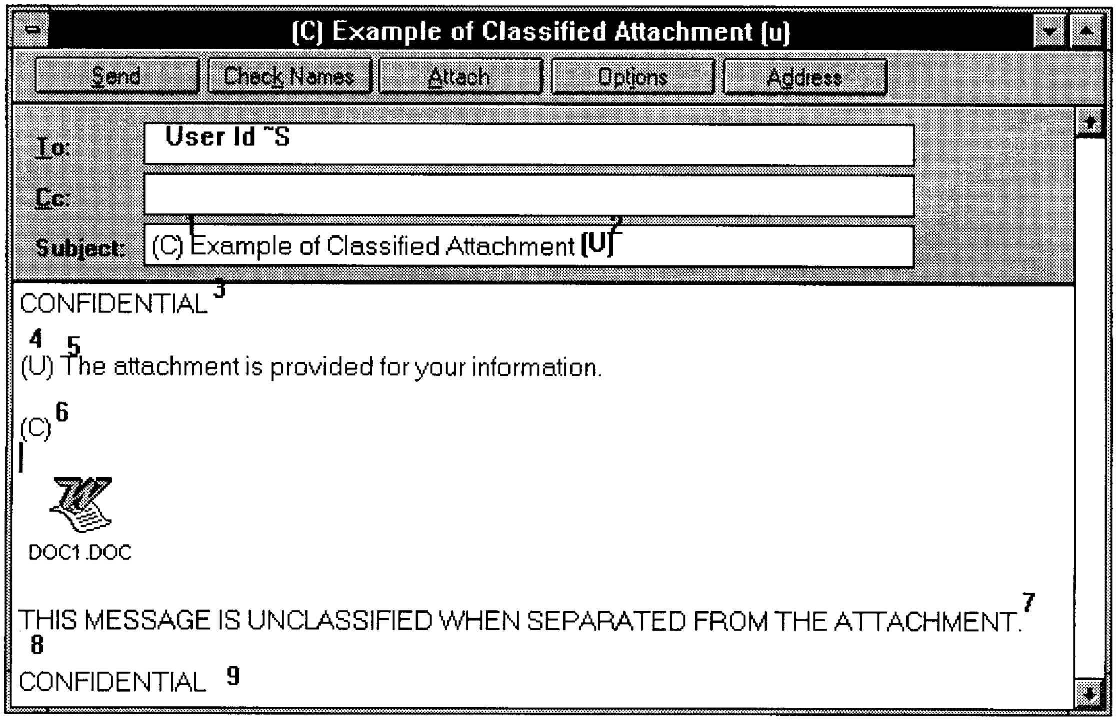
9. Classified by and declassification or downgrading instructions

10. Last Line of Text: Overall classification.

ATTACHING A CLASSIFIED ATTACHMENT

NOTE: Figure A4.1 is unclassified; security markings are for instructional purposes only.

Figure A4.1. Example of E-mail Message with Classified Attachment.



(C) Example of Classified Attachment (u)

To: User Id ˜S

Cc:

Subject: (C) Example of Classified Attachment (U)

CONFIDENTIAL

(U) The attachment is provided for your information.

(C)

DOC1.DOC

THIS MESSAGE IS UNCLASSIFIED WHEN SEPARATED FROM THE ATTACHMENT.

CONFIDENTIAL

NOTES:

1. Subject Line, First Entry: Appropriate classification symbol for the overall classification of e-mail transmission.

2. Subject classification symbol (classified message).

3. Text Box, First Line: Overall classification of e-mail message and attachments.

4. One blank line between classification and message text.

5. Paragraph classification symbols (classified message).

6. Attachment classification symbol.

7. Caveat for classification when e-mail message is separated from the attachment.

8. One blank line between text and classification.

9. Last Line of Text: Overall classification.

TRANSMITTING UNCLASSIFIED INFORMATION ON CLASSIFIED NETWORKS

A5.1. Use the following guidelines for all unclassified e-mail sent across any network cleared for classified material:

A5.1.1. Mark unclassified e-mail messages sent across classified networks by entering the symbol "(U)" in parenthesis as the first marking in the "Subject" box of the message.

A5.1.2. Place the word UNCLASSIFIED in uppercase letters as the first line of the e-mail text. Include no other text on this line.

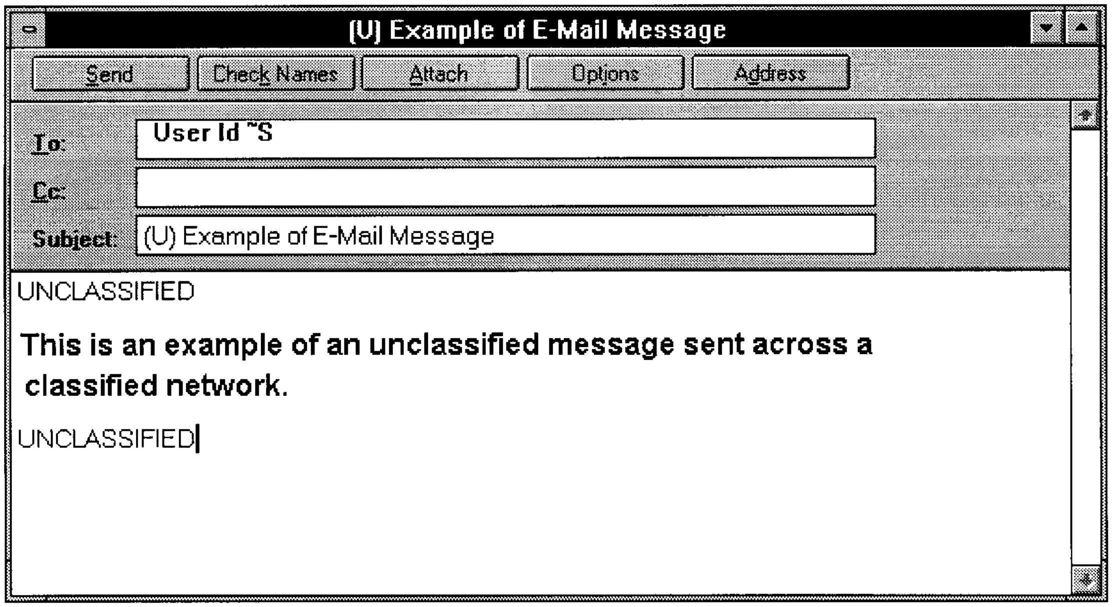
A5.1.3. Begin the text of the message on the third line (that is, one blank line between UNCLASSIFIED and the beginning of the e-mail message text).

A5.1.4. Place the word UNCLASSIFIED in uppercase letters two lines below the last line of the message text (that is, one blank line between "UNCLASSIFIED" and the last line of the e-mail message). Include no other text on this line.

A5.1.5. Attachments included in an unclassified e-mail transmission do not need to have the classification noted.

NOTE: If an attachment is classified, the entire e-mail transmission is classified.

Figure A5.1. Example of Unclassified E-mail Sent Across a Classified Network.



(U) Example of E-Mail Message

To: User Id ˜S

Cc:

Subject: (U) Example of E-Mail Message

UNCLASSIFIED

This is an example of an unclassified message sent across a classified network.

UNCLASSIFIED